UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

JANNIA BARNES, on behalf of herself and all others similarly situated, Plaintiff, v. M&D CAPITAL PREMIER BILLING, LLC, Defendant.	**Case No. 24-cv-2543** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jannia Barnes ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against M&D Capital Premier Billing, LLC ("M&D Billing" or "Defendant"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information that Plaintiff and Class Members entrusted to it, including, without limitation: names, Social Security numbers, financial information, addresses, medical billing and insurance information, medical information, and demographic information.[1]

2. M&D Billing describes itself as a "specialty healthcare advisory firm that assists healthcare providers to grow their businesses. Our principals have deep experience in managing the complicated financial affairs of medical practices…. In our extensive experience billing and

[1] https://oag.ca.gov/system/files/MD%20-%20Letter%20to%20Patients%20%28general%29%20-%20Redacted%20Proof%284085005.1%29.pdf (last accessed April 3, 2024).

collecting for our clients, M&D Capital has developed unique tools that enable us to get higher reimbursements faster and with less hassle."[2]

3. M&D Billing is related to companies ASC Strategic Services LLC and Drachman Katz LLP.[3]

4. On or around July 8, 2023, M&D Billing identified suspicious activity on its computer network (the "Data Breach").[4] Through its own investigation, M&D "determined that an unauthorized threat actor may have had access to certain systems beginning on or around June 20, 2023."[5] Consequently, according to M&D, "certain files within our systems may have been accessed or acquired by the unauthorized threat actor."[6]

5. Upon information and belief, during the Data Breach, the attacker compromised the personally identifiable information[7] ("PII") and protected health information ("PHI") (collectively, "Personal Information") of the customers of all the companies the Defendant was providing services to.

6. On or around March 18, 2024, more than seven months after Defendant became aware of the suspicious activity, Defendant began sending breach notification letters notifying Plaintiff and Class Members of the Data Breach and cautioned them to review their healthcare statements for instances of fraud.[8]

---

[2] https://mdcapitalbilling.com/about-us/ (last accessed April 3, 2024).
[3] https://newstral.com/en/article/en/1251329383/m-d-capital-premier-billing-notifies-consumers-of-june-2023-data-breach (last accessed April 3, 2024).
[4] https://oag.ca.gov/system/files/MD%20-%20Letter%20to%20Patients%20%28general%29%20-%20Redacted%20Proof%284085005.1%29.pdf (last accessed April 3, 2024).
[5] *Id.*
[6] *Id.*
[7] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).
[8] *Notice of Data Breach*, supra. Exhibit 1.

7. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Personal Information, Defendant assumed legal and equitable duties to those individuals.

8. The exposed Personal Information of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted Personal Information to criminals. As already acknowledged by Defendant, Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

9. This Personal Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Personal Information of Plaintiff and Class Members.

10. Plaintiff brings this action on behalf of all persons whose Personal Information was compromised as a result of Defendant's failure to: (i) adequately protect the Personal Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the Personal Information of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of their Personal Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their Personal

Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information; (c) likely remains freely available for cybercriminals to use and abuse

12. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' Personal Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the Personal Information of Plaintiff and Class Members was compromised through disclosure to and exfiltration by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Jannia Barnes is a citizen of Pennsylvania, residing in Philadelphia, Pennsylvania. Plaintiff was, at all relevant times, a patient of one of Defendant's clients whose Personal Information was retained on Defendant's systems.

14. On or about March 21, 2024, Plaintiff received a Notice of Data Breach in the mail from Defendant.

15. Defendant M&D Capital Premier Billing, LLC is a medical servicing company with its principal place of business located at 115-06 Myrtle Avenue, Richmond Hill, New York, 11418.

16. Upon information and belief, Defendant M&D Capital Premier Billing, LLC employs more than 25 people and generates approximately $5 million in annual revenue.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

18. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. Section 1332(d) in that (1) this is a class action involving more than 100 class members; (2) Plaintiff is a citizen of Pennsylvania and Defendant is a citizen of New York and/or avail itself to the subject matter jurisdiction of the State of New York, thus there is minimal diversity because Plaintiff and Defendant are citizens of different states; and (3) the amount in controversy is in excess of $5,000,000, exclusive of interests and costs.

20. Defendant is subject to the personal jurisdiction of this Court because Defendant resides in this county. Additionally, the Defendant regularly and systematically conducts business and provides medical care in this county. Defendant also regularly and systematically collects and stores personal and medical information while providing services to individuals in this county, including Plaintiff and members of the putative Class.

21. Venue is appropriate here under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

22. Defendant M&D Capital Premier Billing LLC is a medical services provider based in Richmond Hill, New York.

23. Defendant collects and stores some of Plaintiff's and Class Members' most sensitive and confidential information, including their Social Security numbers, medical billing and insurance information, personal medication and treatment information, and financial information, as a condition of rendering medical services.[9]

24. Plaintiff and Class Members relied on this sophisticated Defendant's promises to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their Personal Information.

25. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' Personal Information from involuntary disclosure to third parties.

26. The healthcare sector is a favored target by cybercriminals, yet recent studies, including one by the Massachusetts Institute of Technology, found medical centers lagged behind other businesses in safeguarding their computer systems.[10] A Tenable study analyzing healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."[11]

---

[9] https://oag.ca.gov/system/files/MD%20-%20Letter%20to%20Patients%20%28general%29%20-%20Redacted%20Proof%284085005.1%29.pdf (last accessed April 3, 2024).

[10] Jane Musgrave, *How two Palm Beach County Hospitals used paper to cope with a cyber attack,* PALM BEACH POST (Apr. 30, 2022), https://www.palmbeachpost.com/story/news/healthcare/2022/04/30/west-palm-beach-hospitals-handle-cyber-attack-ransomware-hive/9575400002/. (last accessed April 3, 2024).

[11] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches. (last accessed April 3, 2024).

27. As a result of Defendant's failure to implement and follow basic security procedures, the Personal Information of Plaintiff and Class Members was more likely than not accessed, disclosed, and/or acquired and is now in the hands of criminals.

28. Once information is placed onto the internet, it is virtually impossible to remove. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Defendant's failures.

29. Additionally, as a result of Defendant's failure to follow industry standard security procedures, Plaintiff and Class Members received only a diminished value of the services Defendant was to provide.

30. By obtaining, collecting, using, and deriving a benefit from the Personal Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access, intrusion, and/or acquisition.

31. Moreover, Defendant now puts the burden squarely on Plaintiff and Class Members to enroll in the credit monitoring services, among other steps Plaintiff and Class Members must take to protect themselves. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[12]

32. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per

[12] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, *available at* https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed April 3, 2024).

week;[13] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[14] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

33. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

The Data Breach

34. On or about March 18, 2024, Defendant sent out notices to individuals like Plaintiff and Class Members ("Notice of Data Security Incident"). The Notice of Data Security Incident read, in part:

> On or around July 8, 2023, we identified suspicious activity within our computer environment. We immediately took steps to secure our network and launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. Through the investigation, we determined that an unauthorized threat actor may have had access to certain systems beginning on or around June 20, 2023. As a result, certain files within our systems may have been accessed or acquired by the unauthorized threat actor. Based on the investigation we determined that your data may have been included on the impacted systems.
>
> The impacted systems contained demographic and healthcare information provided by the Covered Entity, which may include your name, address, medical billing and insurance information, certain medical information such as diagnoses, medication and treatments, and demographic information such as date of birth, Social Security number and financial information….

[13] *See* https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (last accessed April 3, 2024).
[14] *Id.*

> M&D and the M&D Entities provides medical billing and related services to medical providers. If you received this letter, M&D provides services to one of your medical providers.[15]

35. In response to the Data Breach, Defendant claims that it "promptly notified law enforcement and took steps to further secure our systems and investigate the event. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional administrative and technical safeguards to help prevent future attacks."[16]

36. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing their Personal Information to be exposed.

38. To prevent and detect network server intrusions, Defendant could and should have implemented, as recommended by the United States Government, the following non-exhaustive list of measures:

- Utilize strict access controls, remove backdoor connections, and limit virtual private networks.
- Maintain adequate file system and boot management, stay updated with vendor-supported software, and verify software and configuration settings.
- Use centralized servers, configure authentication, authorization, and

[15] https://oag.ca.gov/system/files/MD%20-%20Letter%20to%20Patients%20%28general%29%20-%20Redacted%20Proof%284085005.1%29.pdf (last accessed April 3, 2024).
[16] *Id.*

accounting, implement the principle of 'least privilege.

- Incorporate specific usernames and account settings, change default passwords, eliminate unnecessary accounts, and store passwords with safe algorithms.
- Configure logging and centralized remote log servers, obtain necessary log information, and synchronize clocks.
- Refrain from using cleartext services, verify appropriate encryption strength, use secure protocols, restrict access to services, and turn off unneeded network services.
- Turn off Internet Protocol service routing and turn on routing authentication.
- Enable port security and disable default virtual local area networks, unused ports, port monitoring, and proxy Address Resolution Protocol.[17]

39. Given that Defendant was storing the Personal Information of the patients of the healthcare entities it was providing services to, Defendant could and should have implemented all the above measures to prevent and detect network server intrusions.

40. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent network server intrusions, resulting in the Data Breach and the exposure of the PII of individuals like Plaintiff and Class Members.

The Healthcare Sector is Particularly Vulnerable to Cyber Attacks

41. Defendant was on notice that companies in the healthcare industry are targets for data breaches.

42. Defendant was on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic

[17] *Network Infrastructure Security Guide*, Nat'l Sec. Agency, https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF. (last accessed April 3, 2024).

rise in cyberattacks, urging facilities to shore up their cyber defenses.[18] Indeed, just days before, HHS's cybersecurity arm issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[19]

43. In the context of data breaches, healthcare is "by far the most affected industry sector."[20] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[21] A Tenable study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in *nearly 93% of the breaches*."[22]

44. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[23]

---

[18] Rebecca Pifer, *Tenet says 'cybersecurity incident' disrupted hospital operations*, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-says-cybersecurity-incident-disrupted-hospital-operations/622692/. (last accessed April 3, 2024).

[19] *Id.* (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

[20] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed April 3, 2024).

[21] *See id.*

[22] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches. (last accessed April 3, 2024).

[23] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last accessed April 3, 2024).

45. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[24]

46. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[25] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[26] That trend continues.

47. The healthcare sector consistently reports one of the highest number of breaches among all measured sectors, with the highest rate of exposure per breach.[27] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[28] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were

---

[24] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last accessed April 3, 2024).

[25] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last accessed April 3, 2024).

[26] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last accessed April 3, 2024).

[27] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last accessed April 3, 2024).

[28] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed April 3, 2024).

never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[29]

48. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[30]

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Personal Information.

49. In the course of its regular business operations, Defendant acquired, collected, and stored Plaintiff's and Class Members' Personal Information.

50. As a condition of its relationships with Plaintiff and Class Members and Defendant's clients, Defendant required that Plaintiff and Class Members entrust Defendant with highly confidential PII.

51. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Personal Information from disclosure.

52. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Personal Information and relied on Defendant to keep their Personal Information confidential and securely maintained, to use this information for business purposes

[29] *Id.*
[30] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks. (last accessed March 28, 2024).

only, and to make only authorized disclosures of this information.

53. Yet, despite the prevalence of public announcements of these data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class Members' Personal Information from being compromised.

Securing PII and Preventing Breaches

54. Defendant could have prevented this Data Breach by properly securing its networks and encrypting the Personal Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data.

55. Defendant's negligence in safeguarding the Personal Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

56. Indeed, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Personal Information of Plaintiff and Class Members from being compromised.

57. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[31] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[32]

58. The ramifications of Defendant's failure to keep secure the Personal Information

[31] 17 C.F.R. § 248.201 (2013).
[32] *Id.*

of Plaintiff and Class Members are long lasting and severe. Once stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

59. The Personal Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[33] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[34] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[35]

60. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number

[33] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed April 3, 2024).
[34] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed April 3, 2024).
[35] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed April 3, 2024).

and assuming your identity can cause a lot of problems.[36]

61. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[37]

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and potentially date of birth.

64. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[38]

---

[36] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed April 3, 2024).

[37] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed April 3, 2024).

[38] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed April 3, 2024).

65. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

66. The Personal Information of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the Personal Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

67. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[39]

68. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Personal Information of Plaintiff and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the Personal Information was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

69. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

[39] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last accessed April 3, 2024).

70. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

71. To date, Defendant has offered credit monitoring services only "for twelve months from the date of enrollment when changes occur to your credit file."[40]

72. Further, there is a market for Plaintiff's and Class Members PHI, and the stolen PHI has inherent value.

73. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

74. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to

[40] https://oag.ca.gov/system/files/MD%20-%20Letter%20to%20Patients%20%28general%29%20-%20Redacted%20Proof%284085005.1%29.pdf (last accessed April 3, 2024).

their personal medical files due to the thief's activities."[41]

75. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Personal Information of Plaintiff and Class Members.

Defendant's Conduct Violates the Rules and Regulations of HIPAA and HITECH

76. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

77. Defendant is a covered entity pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

78. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH").[42] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

79. Plaintiff's and Class Members' Personal Information is "protected health information" as defined by 45 CFR § 160.103.

80. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

81. 45 CFR § 164.402 defines "unsecured protected health information" as "protected

[41] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), *available at* https://khn.org/news/rise-of-indentity-theft/ (last accessed April 3, 2024).
[42] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

82. Plaintiff's and Class Members' Personal Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

83. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

84. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

85. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

86. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

87. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

88. The Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of Personal

Information when it was no longer necessary and/or had honored its obligations to Plaintiff and Class Members.

89. It can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff and Class Members' Personal Information.

90. Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502,et seq.; and

k. Retaining information past a recognized purpose and not deleting it.

91. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

92. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiff and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the Personal Information of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' Personal Information remains at risk of subsequent data breaches.

Plaintiff's Experience

93. Plaintiff learned of the Data Breach when she received her Notice of Data Breach, which was dated March 21, 2024. The Notice informed Plaintiff that her Personal Information was compromised in the Data Breach.

94. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach. This time has been lost forever and cannot be recaptured.

95. Plaintiff has taken it upon herself to research and investigate the Data Breach, check her bank account daily, and is placing a freeze on her credit reports. Plaintiff is incredibly afraid that a bad actor will use her private information to negatively impact her credit as a result of this Data Breach.

96. Upon information and belief, Plaintiff's Personal Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

97. As the result of an injury, Plaintiff visited one of Defendant's clients for medical care and provided the client with her Social Security number, date of birth, address, and medical and healthcare information, including, but not limited to, her prior diagnoses, medications, treatments, and billing and insurance information. Ultimately, her information ended up in the Defendant's possession and is now forever exposed.

98. Plaintiff has been receiving a major increase in both spam and repeated text messages from UPS, notifications regarding prescriptions Plaintiff never ordered, and numerous messages from Citizens Bank. Out of an abundance of caution, Plaintiff reached out directly to Citizens Bank – a bank she never did business with – to ensure that no accounts were opened in her name.

99. Plaintiff is applying for the credit protection offered in the Notice, but states that it is "not nearly enough" to protect her data.

100. Plaintiff is very careful about sharing her Personal Information. She has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff stores any documents containing her Personal Information in a safe and secure

location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

101. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving medical care from Defendant, which was compromised in and as a result of the Data Breach.

102. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

103. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her Personal Information, especially her Social Security number, in combination with her name, being placed in the hands of unauthorized third parties and criminals.

104. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's Personal Information. Plaintiff has expressed tremendous discontent with the fact that it took the Defendant ***more than seven months*** to inform her that she was a victim of the Data Breach. Had Plaintiff received immediate notification, a number of the nefarious and suspicious activities that have taken place – and very possibly will persist – on her accounts could have been avoided or mitigated.

105. Plaintiff has a continuing interest in ensuring that her Personal Information, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

106. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), *et seq*.

and other applicable law.

107. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose Personal Information was compromised during the Data Breach referenced in M&D Capital Premier Billing's Notice of Data Security Incident published by Defendant on or around March 18, 2024 (the "Nationwide Class").

108. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate subclass, defined as follows:

> All individuals residing in New York whose Personal Information was compromised during the Data Breach referenced in the Notice of Data Security Incident published by Defendant on or around March 18, 2024 (the "New York Class").

109. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

110. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

111. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class-wide relief because Plaintiff and all members of the Nationwide Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

112. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Federal Rule of Civil Procedure 23.

113. The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least thousands of Class Members.

114. Common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the Personal Information of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the Personal Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Personal Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Personal Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Personal Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Personal Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in

the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Personal Information of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

115. Plaintiff is a member of the Classes he seeks to represent, and her claims and injuries are typical of the claims and injuries of the other Class Members.

116. Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiff and her counsel.

117. Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

118. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims

in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

119. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

120. Plaintiff and the Nationwide Class provided and entrusted Defendant and Defendant's clients with certain Personal Information as a condition of receiving medical services and care based upon the premise and with the understanding that Defendant would safeguard their information, use their Personal Information for business purposes only, and/or not disclose their Personal Information to unauthorized third parties.

121. Defendant has full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the Personal Information were wrongfully disclosed.

122. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Personal Information of Plaintiff and the

Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

123. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Personal Information of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

124. Defendant owed a duty to Plaintiff and the Nationwide Class to implement intrusion detection processes that would detect a data breach or unauthorized access to its systems in a timely manner.

125. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Personal Information it was no longer required to retain pursuant to regulations, including that of former patients.

126. Defendant also had a duty to employ proper procedures to detect and prevent the improper access, misuse, acquisition, and/or dissemination of the Personal Information of Plaintiff and the Nationwide Class.

127. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant and Defendant's clients with their confidential Personal Information, a necessary part of their relationships with Defendant.

128. Defendant owed a duty to disclose the material fact that Defendant's data security practices were inadequate to safeguard the personal and medical information of Plaintiff and the

Nationwide Class.

129. Defendant's Privacy Policies acknowledge Defendant's duty to adequately protect the personal and medical information of Plaintiff and the Nationwide Class.

130. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

131. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting Personal Information stored on Defendant's systems.

132. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Personal Information of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

133. Plaintiff and the Nationwide Class had no ability to protect their Personal Information that was in, and likely remains in, Defendant's possession.

134. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

135. Defendant had and continues to have a duty to adequately disclose that the Personal Information of Plaintiff and the Nationwide Class within Defendant's possession was

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal Information by third parties.

136. Defendant has admitted that the Personal Information of Plaintiff and the Nationwide Class was wrongfully accessed, acquired, and/or released to unauthorized third persons as a result of the Data Breach.

137. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Personal Information of Plaintiff and the Nationwide Class during the time the Personal Information was within Defendant's possession or control.

138. Defendant improperly and inadequately safeguarded the Personal Information of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

139. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Personal Information of Plaintiff and the Nationwide Class in the face of increased risk of theft.

140. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect unauthorized access or intrusions and prevent dissemination of their Personal Information. Additionally, Defendant failed to disclose to Plaintiff and the Nationwide Class that Defendant's security practices were inadequate to safeguard the Personal Information of Plaintiff and the

Nationwide Class.

141. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Personal Information it was no longer required to retain pursuant to regulations, including Personal Information of former patients.

142. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

143. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Personal Information of Plaintiff and the Nationwide Class would not have been compromised.

144. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal Information of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Personal Information of Plaintiff and the Nationwide Class was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personal Information by adopting, implementing, and maintaining appropriate security measures.

145. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer injury.

146. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

147. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

148. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

149. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

150. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

151. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

152. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

153. The harm that occurred because of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

154. Defendant's violations of HIPAA and HITECH also independently constitute

negligence *per se*.

155. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

156. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

157. The harm that occurred because of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

158. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Personal Information is used; iii) the compromise, publication, and/or theft of their Personal Information ; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information ; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Personal Information, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal

Information of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

159. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

160. Defendant required Plaintiff and the Nationwide Class to provide and entrust their Personal Information as a condition of obtaining medical care from Defendant's clients.

161. Plaintiff and the Nationwide Class paid money to Defendant's clients in exchange for goods and services, as well as Defendant's promises to protect their protected health information and other Personal Information from unauthorized disclosure.

162. In its written Privacy Policy, Defendant expressly promised Plaintiff and Class Members that Defendant would only disclose Personal Information under certain circumstances, none of which relate to the Data Breach.

163. Defendant promised to comply with HIPAA and HITECH standards and to make sure that Plaintiff's and Class Members' Personal Information would remain protected.

164. As a condition of obtaining medical care from Defendant's clients, Plaintiff and the Nationwide Class provided and entrusted their Personal Information. In so doing, Plaintiff the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to

timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

165. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete Personal Information and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their Personal Information.

166. Plaintiff and the Nationwide Class Members would not have entrusted their Personal Information to Defendant in the absence of Defendant's implied promise to adequately safeguard this confidential personal and medical information.

167. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

168. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by making their Personal Information accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the Personal Information was secure, failing to encrypt Plaintiff and Class Members' sensitive Personal Information, failing to safeguard and protect their Personal Information, and by failing to provide timely and accurate notice to them that Personal Information was compromised as a result of the data breach.

169. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to comply with its promise to abide by HIPAA and HITECH.

170. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

171. Defendant further breached the implied contracts with Plaintiff and Class Members

by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

172. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

173. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

174. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

175. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

176. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

177. Defendant further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

178. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

179. Defendant further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Personal Information.

180. Defendant's failures to meet these promises constitute breaches of the implied contracts.

181. Because Defendant allowed unauthorized access to Plaintiff and Class Members' Personal Information and failed to safeguard the Personal Information, Defendant breached its contracts with Plaintiff and Class Members.

182. Defendant breached its contracts by not meeting the minimum level of protection of Plaintiff and Class Members' protected health information and other Personal Information, because Defendant did not take appropriate measures to prevent the Data Breach from occurring.

183. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiff and Class Members that were of a diminished value.

184. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class are now subject to the present and continuing risk of fraud, and are suffering (and will continue to suffer) the ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the diminished value of services provided by

Defendant; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

185. As a result of Defendant's breach of implied contract, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class)

186. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

187. At all times during Plaintiff's and the Nationwide Class's interactions with Defendant, as a healthcare related entity, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Nationwide Class's Personal Information that Plaintiff and the Nationwide Class provided to Defendant.

188. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff and the Nationwide Class's Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

189. Plaintiff and the Nationwide Class provided their Personal Information to Defendant and Defendant's clients with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

190. Plaintiff and the Nationwide Class also provided their PII to Defendant and Defendant's clients with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

191. Defendant voluntarily received in confidence the PII of Plaintiff and the Nationwide Class with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

192. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII of Plaintiff and the Nationwide Class was disclosed and misappropriated to unauthorized third parties beyond Plaintiff and the Nationwide Class's confidence, and without their express permission.

193. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

194. But for Defendant's disclosure of Plaintiff and the Nationwide Class's Personal Information in violation of the parties' understanding of confidence, their Personal Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff and the Nationwide Class's Personal Information as well as the resulting damages.

195. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff and the Nationwide Class's Personal Information. Defendant knew or should have known its methods of accepting and securing Plaintiff and the Nationwide Class's Personal Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff and the Nationwide Class's Personal Information.

196. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

197. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

198. As a result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT V
VIOLATION OF THE NEW YORK CONSUMER LAW FOR DECEPTIVE ACTS AND PRACTICES ACT
N.Y. Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, on behalf of Plaintiff and the New York Subclass)

199. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

200. The New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

201. By reason of the conduct alleged herein, Defendant has engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

202. Defendant stored Plaintiff's and Class Members' Personal Information on the aforementioned servers. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiff's and Class Members' Personal Information secure and prevented the loss or misuse of Plaintiff's and Class Members' PII.

203. Plaintiff and Class Members never would have provided their sensitive and Personal Information to Defendant or Defendant's clients if they had been told or knew that Defendant would fail to maintain sufficient security to keep such Personal Information from being taken by others.

204. Defendant violated NYGBL § 349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendant's storage and services, specifically the security thereof, and its ability to safely store and dispose of Plaintiff's and Class Members' Personal Information.

205. Defendant also violated NYGBL § 349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiff and Class Members of the Data Breach. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach.

206. Defendant's practices, acts, policies, and course of conduct violate NYGBL § 349 in that:

a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and Class Members at the time they provided such Personal Information that Defendant did not have sufficient security or mechanisms to protect Personal Information; and

b. Defendant failed to give timely warnings and notices regarding the defects and problems with the security of their computer systems to protect Plaintiff's and Class Members' Personal Information. Defendant possessed actual knowledge of the inherent risks in inadequate data security.

207. Plaintiff and the Class were entitled to assume, and did assume, Defendant would take appropriate measures to keep their Personal Information safe. Defendant did not disclose that Plaintiff's and Class Members' Personal Information was vulnerable to malicious actors, and

Defendant was the only one in possession of that material information, which it had a duty to disclose.

208. The aforementioned conduct constitutes an unconscionable commercial practice in that Defendant has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the inadequate nature of its security practices, resulting in the Data Breach.

209. Members of the public were deceived by Defendant's misrepresentations and failures to disclose.

210. Such acts by Defendant are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Personal Information to Defendant. Said deceptive acts and practices are material. The requests for and use of such Personal Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

211. Defendant's wrongful conduct caused Plaintiff and Class Members to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the Personal Information by third parties and placing Plaintiff and Class Members at serious risk for monetary damages.

212. As a direct and proximate result of Defendant's violations of the above, Plaintiff and Class Members suffered damages including, but not limited to: unauthorized use of their Personal Information; theft of their personal and financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; damages arising from the inability to use their Personal Information; costs associated with time spent and

the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach; the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals; damages to and diminution in value of their Personal Information entrusted to Defendant; and the loss of Plaintiff's and Class Members' privacy.

213. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the Class seek statutory damages for each injury and violation which has occurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the New York Class, and appointing Plaintiff and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts

described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Personal Information of Plaintiff and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of their confidential personal

identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, nominal, and statutory damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, by counsel, hereby demands that this matter be tried before a jury.

Date: April 4, 2024

By: */s/James M. Evangelista*

James M. Evangelista
Evangelista Worley LLC
10 Glenlake Parkway, Suite 130
Atlanta, GA 30328
(404) 205-8400
jim@ewlawllc.com

Jennifer Czeisler
Edward Ciolko
(Pro Hac Vice application forthcoming)
Sterlington, PLLC
One World Trade Center
85th Floor
New York, NY 10007
(516) 457-9571
jen.czeisler@sterlingtonlaw.com
edward.ciolko@sterlingtonlaw.com

Jean S. Martin
(*Pro Hac Vice application forthcoming*)
Francesca K. Burne
(*Pro Hac Vice application forthcoming*)
Morgan & Morgan Complex Litigation Group
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com
fburrne@ForThePeople.com

Attorneys for Plaintiff and the Putative Class